In the Claims:

Cancel claims 1-62 and enter the following new claims.

-- 63. A method for computer-aided interchange of cryptographic keys between a first computer unit and a second computer unit, which comprises:

in the first computer unit, forming a first value from a first random number using a generating element of a finite group;

transmitting a first message, which at least contains the first value, from the first computer unit to the second computer unit;

in the second computer unit, forming a session key using a first hash function; a first input variable for the first hash function including at least one first term that is formed by exponentiation of the first value using a secret network key;

in the first computer unit, forming the session key using the first hash function; a second input variable for the first hash function including at least one second term that is formed by exponentiation of a public network key using the first random number;

in the first computer unit, forming a fourth input variable using a given hash function selected from the group consisting of the first hash function and a second hash function; a third input variable for the given hash function including, for forming the fourth input variable, at least one variable that can be used to unambiguously infer the session key, at least part of the at least one variable being a nonpublic variable;

in the first computer unit, using a first signature function to form a signature term from at least the fourth input variable;

transmitting a third message, which at least includes the signature term, from the first computer unit to the second computer unit; and

in the second computer unit, verifying the signature term.

64. The method according to claim 63, which comprises providing a key selected from the group consisting of the secret network key and the public network key as a long-service key.

65. The method according to claim 63, wherein the third input variable includes a plurality of variables that can be used to unambiguously infer the session key.

66. The method according to claim 63, wherein the at least one variable includes a feature selected from the group consisting of the first value and the public network key.

67. The method according to claim 63, which comprises:

providing a certification computer unit that delivers a network certificate that can be verified by the first computer unit;

providing the first message with an identity statement for the certification computer unit;

transmitting a second message, which includes the network certificate, from the second computer unit to the first computer unit; and

verifying the network certificate in the first computer unit.

68. The method according to claim 67, wherein:

the second message includes a chain of network certificates that have been delivered by the certification computer unit;

a final certificate in the chain of the network certificates is the network certificate; and

the chain of the network certificates is verified in the first computer unit.

69. The method according to claim 67, which comprises:

transmitting a third message, which includes a user certificate, from the first computer unit to the second computer unit;

verifying the user certificate in the second computer unit.

70. The method according to claim 69, wherein:

the third message includes a chain of network certificates;

a final certificate in the chain of the network certificates is the network certificate; and

the chain of the network certificates is verified in the second computer unit.

71. The method according to claim 63, which comprises:

providing a certification computer unit that delivers a network certificate to the first computer unit for verification by the first computer unit;

providing the first message with an identity variable for the first computer unit and with an identity statement for the certification computer unit;

transmitting a fourth message, which includes the first value as an input variable, from the second computer unit to the certification computer unit;

providing a fifth message with a feature selected from the group consisting of the network certificate, a certificate chain including a final element defining the network certificate, a user certificate, and a certificate chain including a final element defining the user certificate; and

transmitting the fifth message from the certification computer unit to the second computer unit.

72. The method according to claim 71, which comprises:

in the first computer unit and before forming the first message, forming an intermediate key by raising a public key

declaration key to a higher power using the first random number;

in the first computer unit and before forming the first message, forming a second encrypted term from the identity variable for the first computer unit by encrypting the identity variable with the intermediate key using an encryption function;

providing the first message with the second encrypted term instead of the identity variable for the first computer unit; and

providing the fourth message with the second encrypted term instead of the identity variable for the first computer unit.

73. The method according to claim 71, which comprises:

providing the fifth message with an encrypted certificate that is encrypted with L; and

selecting the encrypted certificate from the group consisting of the network certificate, the certificate chain including the final element defining the network certificate, the user certificate, and the certificate chain including the final element defining the user certificate.

74. The method according claim 71, which comprises:

in the certification computer unit, using a revocation list to check an element selected from the group consisting of the at least one variable, an identity statement for the second computer unit, the identity variable for the first computer unit, a public network key, the network certificate, and the user certificate.

75. The method according to claim 63, which comprises:

providing a fourth message with at least the public network key, the first value, an identity variable for the first computer unit that is an input variable, and an output variable from a third hash function that is signed using a second signature function;

transmitting the fourth message from the second computer unit to a certification computer unit;

verifying a first signed term in a certification computer unit;

forming a third term in the certification computer unit;

providing the third term with at least the first value, the public network key, and an identity statement for the second computer unit;

forming a hash value for the third term in the certification computer unit using a fourth hash function;

obtaining a signed hash value by signing the hash value for the third term in the certification computer unit using a third signature function;

in the certification computer unit, forming a network certificate containing at least the third term and the signed hash value for the third term;

in the certification computer unit, applying a fourth hash function to a fifth term that includes at least the identity statement for the second computer unit and a user certificate;

obtaining a second signed term by signing a hash value for the fifth term using a secret certification key and the third signature function;

providing a fifth message with at least the network certificate, the fifth term, and the second signed term;

transmitting the fifth message from the certification computer unit to the second computer unit;

verifying the network certificate and the second signed term in the second computer unit;

in the second computer unit, forming a fourth term that includes at least the public network key and the signed hash value for the third term;

transmitting a second message, which at least includes the fourth term, from the second computer unit to the first computer unit; and

verifying the network certificate in the first computer unit.

76. The method according to claim 63, which comprises:

providing a certification computer unit that delivers a network certificate to the first computer unit for verification by the first computer unit;

providing the first message with an identity variable for the first computer unit and with an identity statement for the certification computer unit;

providing a fourth message with at least one certificate for a public network key, the first value, and the identity variable for the first computer unit;

transmitting the fourth message from the second computer unit to the certification computer unit;

in the certification computer unit, forming a third term that includes an element selected from the group consisting of the public network key, and a variable that unambiguously determines the public network key;

in the certification computer unit, forming a hash value for the third term using a fourth hash function;

in the certification computer unit, obtaining a signed hash value by using a third signature function to sign the hash value for the third term;

transmitting a fifth message, containing the signed hash value for the third term, from the certification computer unit to the second computer unit;

in the second computer unit, verifying the signed hash value for the third term;

transmitting a second message, which includes the signed hash value for the third term, from the second computer unit to the first computer unit; and

in the first computer unit, verifying the signed hash value for the third term.

77. The method according to claim 76, wherein:

the certification computer unit delivers a chain of certificates to the first computer unit;

a final certificate in the chain of the certificates is the network certificate; and

the chain of the certificates can be verified in the first computer unit.

78. The method according to claim 76, wherein the third term includes an element selected from the group consisting of a public user signature key and a variable that unambiguously determines the user signature key.

79. The method according to claim 76, wherein the fifth message and the second message each have at least one chain of certificates.

80. The method according to claim 76, wherein the third term has a time stamp.

81. The method according to claim 63, which comprises:

providing a fourth message with at least the public network key, the first value, an identity variable for the first computer unit that is an input variable, and an output variable from a third hash function that is signed using a second signature function;

transmitting the fourth message from the second computer unit to a certification computer unit;

verifying a first signed term in a certification computer unit;

forming a third term in the certification computer unit;

providing the third term with at least the first value, the public network key, and an identity statement for the second computer unit;

forming a hash value for the third term in the certification computer unit using a fourth hash function;

obtaining a signed hash value by signing the hash value for the third term in the certification computer unit using a third signature function;

in the certification computer unit, forming a network certificate containing at least the third term and the signed hash value for the third term;

in the certification computer unit, applying a fourth hash function to a fifth term that includes at least the identity statement for the second computer unit, a user certificate, and a time stamp;

obtaining a second signed term by signing a hash value for the fifth term using a secret certification key and the third signature function;

providing a fifth message with at least the network certificate, the fifth term, and the second signed term;

transmitting the fifth message from the certification computer unit to the second computer unit;

verifying the network certificate and the second signed term in the second computer unit;

in the second computer unit, forming a fourth term that includes at least the public network key and the signed hash value for the third term;

transmitting a second message, which at least includes the fourth term, from the second computer unit to the first computer unit; and

verifying the network certificate in the first computer unit.

82. The method according to claim 63, which comprises:

providing the first message with at least one old temporary identity variable for the first computer unit;

in the second computer unit, after the first message has been received and before the second message is formed, forming a new temporary identity variable for the first computer unit;

forming a fifth encrypted term from the new temporary identity variable for the first computer unit by encrypting the new temporary identity variable for the first computer unit with the session key using an encryption function;

providing the second message with at least a fifth encrypted term;

decrypting the fifth encrypted term in the first computer unit after the second message has been received and before forming the fourth input variable;

providing the third input variable with at least the new temporary identity variable for the first computer unit for forming the fourth input variable; and

ensuring that the third message does not contain the identity variable for the first computer unit.

83. The method according to claim 63, which comprises:

in the second computer unit, forming a response containing information about the session key;

transmitting a second message, which includes the response, from the second computer unit to the first computer unit; and

using the response to check the session key in the first computer unit.

84. The method according to claim 63, which comprises providing the third message with an identity variable for the first computer unit.

85. The method according to claim 63, which comprises:

in the second computer unit, providing the first input variable for the first hash function with at least one second random number;

providing the second message with the second random number; and

in the first computer unit, providing the second input variable for the first hash function with at least the second random number.

86. The method according to claim 63, wherein:

the third input variable includes a plurality of variables that can be used to unambiguously infer the session key; and

the plurality of the variables include the second random number.

87. The method according to claim 63, which comprises:

before forming the third message, forming a second encrypted term in the first computer unit by using an encryption function to encrypt an identity variable for the first computer unit with the session key;

providing the third message with the second encrypted term; and

decrypting the second encrypted term in the second computer unit after the third message has been received.

88. The method according to claim 63, which comprises:

providing the second message with an optional first data field; and

providing the third input variable with the optional first data field for forming the fourth input variable.

89. The method according to claim 63, which comprises:

in the first computer unit, before forming the third message, forming a third encrypted term by encrypting at least one optional second data field with the session key using an encryption function;

providing the third message with at least the third encrypted term; and

in the second computer unit, decrypting the third encrypted term after the third message has been received.

90. The method according to claim 63, which comprises:

in the first computer unit, before forming the third message, forming a first encrypted term by at least encrypting the signature term using an encryption function;

providing the third message with the first encrypted term; and

decrypting the first encrypted term in the second computer unit after the third message has been received and before the signature term is verified.

91. The method according to claim 63, which comprises:

in the second computer unit, forming a response by using an encryption function to encrypt a constant, which is known in the second computer unit and the first computer unit, with the session key.

92. The method according to claim 91, which comprises:

in the second computer unit, forming the response by using the encryption function to also encrypt additional variables with the session key.

93. The method according to claim 63, which comprises:

in the first computer unit, checking a response by using an encryption function to encrypt a constant with the session key and comparing a result with the response.

94. The method according to claim 93, which comprises checking the response by using the encryption function to also encrypt additional variables with the session key.

95. The method according to claim 63, which comprises:

in the first computer unit, checking a response by decrypting the response with the session key using an encryption function and comparing a decrypted constant with a constant.

96. The method according to claim 95, which comprises:

in the first computer unit, checking the response by also comparing the decrypted constant with additional variables.

97. The method according to claim 63, which comprises:

forming a response in the second computer unit by applying a third hash function to an input variable that includes the session key; and

in the first computer unit, checking the response by:

applying the third hash function to the input variable that includes the session key to obtain a result, and comparing the result with the response.

98. The method according to claim 63, wherein the third message includes at least one optional second data field.

99. The method according to claim 63, which comprises providing the first computer unit as a mobile communication terminal.

100. The method according to claim 99, which comprises providing the second computer unit as an authentication unit in a mobile communication network.

101. A configuration for computer-aided interchange of cryptographic keys between a first computer unit and a second computer unit, comprising:

a first computer unit and a second computer unit configured such that:

the first computer unit forms a first value from a first random number using a generating element of a finite group,

the first computer unit transmits a first message from the first computer unit to the second computer unit, the first message includes at least the first value,

the second computer unit forms a session key using a first hash function,

a first input variable for the first hash function includes at least one first term formed by exponentiation of the first value using a secret network key,

the first computer unit forms the session key using the first hash function,

a second input variable for the first hash function includes at least one second term formed by exponentiation of a public network key using the first random number,

the first computer unit forms a fourth input variable using a given hash function selected from the group consisting of the first hash function and a second hash function,

a third input variable for the given hash function including, for forming the fourth input variable, at least one variable that can be used to unambiguously infer the session key,

at least part of the at least one variable being a nonpublic variable,

the first computer unit uses a first signature function to form a signature term from at least the fourth input variable,

the first computer unit transmits a third message to the second computer unit, the third message including at least the signature term from the first computer unit, and

the second computer unit verifies the signature term.

102. The configuration according to claim 101, wherein a key selected from the group consisting of the secret network key and the public network key is a long-service key.

103. The configuration according to claim 101, wherein the first computer unit and the second computer unit are configured such that the third input variable includes a plurality of variables that can be used to unambiguously infer the session key.

104. The configuration according to claim 101, wherein the first computer unit and the second computer unit are configured such that the at least one variable includes a feature selected from the group consisting of the first value and the public network key.

105. The configuration according to claim 101, comprising:

a certification computer unit delivering a network certificate that can be verified by the first computer unit;

the first computer unit and the second computer unit being configured such that:

the first message includes an identity statement for the certification computer unit,

the second computer unit transmits a second message to the first computer unit,

the second message includes the network certificate, and

the first computer unit verifies the network certificate.

106. The configuration according to claim 105, wherein:

the certification computer unit delivers a chain of network certificates;

the network certificate is a final certificate in the chain of network certificates;

the second message includes the chain of network certificates; and

the first computer unit verifies the chain of the network certificates.

107. The configuration according to claim 105, wherein the first computer unit and the second computer unit are configured such that:

the first computer unit transmits a third message to the second computer unit;

the third message includes a user certificate; and

the second computer unit verifies the user certificate.

108. The configuration according to claim 107, wherein:

the third message includes a chain of user certificates;

the user certificate is a final certificate in the chain of the user certificates; and

the second computer unit verifies the chain of the user certificates.

109. The configuration according to claim 101, comprising:

a certification computer unit that delivers a network certificate to the first computer unit for verification by the first computer unit;

the first computer unit, the second computer unit, and the certification computer unit being configured such that:

the first message includes an identity variable for the first computer unit and an identity statement for the certification computer unit,

the second computer unit transmits a fourth message to the certification computer unit,

the fourth message includes the first value as an input variable,

the certification computer unit transmits a fifth message to the second computer unit, and

the fifth message includes a feature selected from the group consisting of the network certificate, a certificate chain including a final element defining the network certificate, a user certificate, and a certificate chain including a final element defining the user certificate.

110. The configuration according to claim 109, wherein the first computer unit and the second computer unit are configured such that a fifth term has a time stamp.

111. The configuration according to claim 109, wherein the first computer unit and the second computer unit are configured such that a third term has a time stamp.

112. The configuration according to claim 109, wherein the first computer unit and the second computer unit are configured such that:

before forming the first message, the first computer unit forms an intermediate key by raising a public key declaration key to a higher power using a first random number;

before forming the first message, the first computer unit forms a second encrypted term from the identity variable for the first computer unit by encrypting the identity variable with an intermediate key using an encryption function;

the first message includes a second encrypted term instead of the identity variable for the first computer unit; and

the fourth message includes the second encrypted term instead of the identity variable for the first computer unit.

113. The configuration according to claim 109, wherein:

the feature, which is selected from the group consisting of the network certificate, the certificate chain including the final element defining the network certificate, the user certificate, and the certificate chain including the final element defining the user certificate, is encrypted with L in the fifth message.

114. The configuration according to claim 109, wherein the first computer unit and the second computer unit are configured such that:

the certification computer unit checks an element using a revocation list; and

the element is selected from the group consisting of the at least one variable, an identity statement for the second computer unit, an identity variable for the first computer unit, the public network key, the network certificate, and the user certificate.

115. The configuration according to claim 101, comprising:

a certification computer unit;

the first computer unit, the second computer unit, and the certification computer unit being configured such that:

the second computer unit transmits a fourth message to the certification computer unit,

the fourth message includes the public network key, the first value, an identity variable for the first computer unit provided as an input variable, and an output variable from a third hash function that is signed using a second signature function,

the certification computer unit verifies a first signed term,

the certification computer unit forms a third term,

the third term includes the first value, the public network key and an identity statement for the second computer unit,

the certification computer unit forms a hash value for the third term using a fourth hash function,

the certification computer unit uses a third signature function to sign the hash value for the third term and to thereby obtain a signed hash value,

the certification computer unit forms a network certificate containing the third term and the signed hash value for the third term,

the certification computer unit applies a fourth hash function to a fifth term containing the identity statement for the second computer unit and a user certificate,

a9 a hash value for the fifth term is signed with a secret certification key by using the third signature function and results in a second signed term,

the certification computer unit transmits a fifth message to the second computer unit,

the fifth message includes the network certificate, the fifth term, and the second signed term,

the second computer unit verifies the network certificate and the second signed term,

the second computer unit forms a fourth term including the public network key and the signed hash value for the third term,

the second computer unit transmits a second message to the first computer unit,

the second message includes the fourth term, and

the first computer unit verifies the network certificate.

116. The configuration according to claim 101, comprising:

a certification computer unit that delivers a network certificate to the first computer unit that can be verified by the first computer unit;

the first computer unit, the second computer unit, and the certification computer unit, are configured such that:

a key selected from the group consisting of the secret network key and the public network key is a long-service key; and

the first message includes an identity variable for the first computer unit and an identity statement for the certification computer unit,

the second computer unit transmits a fourth message to the certification computer unit,

the fourth message includes at least one certificate for the public network key, the first value, and an identity variable for the first computer unit,

the certification computer unit forms a third term that includes an element selected from the group consisting of at least one public network key, and a variable that unambiguously determines the public network key,

the certification computer unit uses a fourth hash function to form a hash value for the third term,

the certification computer unit uses a third signature function to sign the hash value for the third term and to thereby obtain a signed hash value,

the certification computer unit transmits a fifth message to the second computer unit,

the fifth message includes the signed hash value for the third term,

the second computer unit verifies the signed hash value for the third term,

the second computer unit transmits a second message to the first computer unit,

the second message includes the signed hash value for the third term, and

a9

the first computer unit verifies the signed hash value for the third term.

117. The configuration according to claim 116, wherein:

the certification computer unit delivers a chain of network certificates that can be verified by the first computer unit; and

the network certificate is a final certificate in the chain of network certificates.

118. The configuration according to claim 116, wherein the first computer unit and the second computer unit are configured such that:

the third term includes a feature selected from the group consisting of a public user signature key and a variable that unambiguously determines the public user signature key.

119. The configuration according to claim 116, wherein the first computer unit and the second computer unit are configured such that the fifth message and the second message include at least one chain of certificates.

120. The configuration according to claim 101, wherein the first computer unit and the second computer unit are configured such that:

the first message includes at least one old temporary identity variable for the first computer unit;

after the first message has been received and before the second message is formed, the second computer unit forms a new temporary identity variable for the first computer unit;

the first computer unit forms a fifth encrypted term from the new temporary identity variable for the first computer unit by

encrypting the new temporary identity variable for the first computer unit with the session key using an encryption function;

the second message includes the fifth encrypted term;

after the second message has been received and before the fourth input variable is formed, the first computer unit decrypts the fifth encrypted term;

the third input variable for the given hash function includes the new temporary identity variable for the first computer unit for forming the fourth input variable; and

the third message does not include an identity variable for the first computer unit.

121. The configuration according to claim 101, wherein the first computer unit and the second computer unit are configured such that:

the second computer unit forms a response including information about the session key;

the second computer unit transmits a second message to the first computer unit;

the second message includes the response; and

the first computer unit checks the session key using the response.

122. The configuration according to claim 101, wherein the first computer unit and the second computer unit are configured such that the third message includes an identity variable for the first computer unit.

123. The configuration according to claim 101, wherein the first computer unit and the second computer unit are configured such that:

in the second computer unit, the first input variable for the first hash function includes a second random number;

the second message includes the second random number; and

in the first computer unit, the second input variable for the first hash function includes the second random number.

124. The configuration according to claim 101, wherein the first computer unit and the second computer unit are configured such that:

the third input variable includes a plurality of variables that can be used to unambiguously infer the session key; and

the plurality of the variables include the second random number.

125. The configuration according to claim 101, wherein the first computer unit and the second computer unit are configured such that:

before the third message is formed, the first computer unit forms a second encrypted term from the identity variable for the first computer unit by using an encryption function to encrypt at least the identity variable with the session key;

the third message includes the second encrypted term; and

the second computer unit decrypts the second encrypted term after the third message has been received.

126. The configuration according to claim 101, wherein the first computer unit and the second computer unit are configured such that:

the second message includes an optional first data field; and

the third input variable for the given hash function includes the optional first data field for forming the fourth input variable.

127. The configuration according to claim 101, wherein the first computer unit and the second computer unit are configured such that:

before the third message is formed, the first computer unit forms a third encrypted term by encrypting an optional second data field with the session key using an encryption function;

the third message includes the third encrypted term; and

after the third message has been received, the second computer unit decrypts the third encrypted term.

128. The configuration according to claim 101, wherein the first computer unit and the second computer unit are configured such that:

before the third message is formed, the first computer unit forms a first encrypted term by at least encrypting the signature term using an encryption function;

the third message includes the first encrypted term; and

after the third message has been received and before the signal term is verified, the second computer unit decrypts the first encrypted term.

129. The configuration according to claim 101, wherein the first computer unit and the second computer unit are configured such that:

the second computer unit forms a response by using an encryption function to encrypt a constant, which is known in the first compute unit and the second computer unit, with the session key.

130. The configuration according to claim 129, wherein the response is formed by also encrypting additional variables, which are known in the first compute unit and the second computer unit, with the session key.

131. The configuration according to claim 129, wherein the first computer unit is configured to check the response by:

using the encryption function to encrypt a constant with the session key to obtain a result; and

comparing the result with the response.

132. The configuration according to claim 131, wherein the first computer unit is configured to check the response by also encrypting additional variables with the session key to obtain the result.

133. The configuration according to claim 129, wherein the first computer unit and the second computer unit are configured such that:

the first computer unit checks the response by:

decrypting the response with the session key using an encryption function to obtain a decrypted constant, and

comparing the decrypted constant with a constant.

134. The configuration according to claim 129, wherein the first computer unit and the second computer unit are configured such that:

the first computer unit checks the response by:

decrypting the response with the session key using an encryption function to obtain a decrypted constant, and

comparing the decrypted constant an additional variables with a constant.

135. The configuration according to claim 101, wherein the first computer unit and the second computer unit are configured such that:

the second computer unit forms a response by applying a third hash function to an input variable that includes the session key; and

the first computer unit checks the response by:

applying the third hash function to an input variable, which includes the session key, to obtain a result, and

comparing the result with the response.

136. The configuration according to claim 101, wherein the first computer unit and the second computer unit are configured such that the third message includes at least one optional second data field.

137. The configuration according to claim 101, wherein the first computer unit is a mobile communication terminal.

138. The configuration according to claim 137, wherein the second computer unit is an authentication unit in a mobile communication network.

139. The configuration according to claim 101, wherein the second computer unit is an authentication unit in a mobile communication network. --